CLAIMS

WE CLAIM:

1. A computer program for identifying malicious portions in a suspect computer program comprising:

a preprocessor portion for receiving the suspect computer program and creating a logically equivalent standardized version of the suspect program;

a library of standardized malicious code portions; and

a detector portion reviewing the standardized version against the library of malicious code portions to provide an output indicating when a malicious code portion is present in the suspect program.

2. The computer program of claim 1 wherein the standardized version identifies the execution order of instructions of the suspect program and wherein the detector portion reviews the instructions of the standardized version according to the execution order.

3. The computer program of claim 2 wherein the preprocessor identifies the execution order of the instructions by generation of a control-flow listing of the instructions.

4. The computer program of claim 1 wherein the standardized version maps instructions of the suspect program to corresponding standard synonym instructions.

5. The computer program of claim 4 wherein the standard synonym instructions are different in number from the instructions of the suspect program to which the synonym instructions map.

6. The computer program of claim 1 wherein the standardized version removes irrelevant portions of the suspect program.

7. The computer program of claim 6 wherein the preprocessor removes irrelevant portions by identifying irrelevant portions to the detector so that the

detector ignores identified irrelevant portions when reviewing the standardized version.

8. The computer program of claim 1 wherein the irrelevant portions are one or more nop instructions.

9. The computer program of claim 1 wherein the standardized version uses uninterpreted variables.

10. The computer program of claim 1 wherein the suspect program is a binary executable and wherein the preprocessor receives the binary executable to generate a listing of instructions and data values.

11. The computer program of claim 1 further including a library of patterns matching to one or more instructions of the suspect program and wherein the preprocessor creates the standardized version by replacing instructions of the suspect program with matching ones of the library of patterns and wherein the library of standardized malicious code portions are also collections of ones of the library of patterns.

12. The computer program of claim 11 wherein a pattern is at least one instruction logically replacing at least one different instruction in the suspect program.

13. The computer program of claim 11 wherein a pattern in a tag replacing at least one instruction logically having no substantive effect on the execution of the suspect program;

a library of patterns is implemented as a look-up table matching instructions to the patterns.

14. The computer program of claim 1 wherein the library of standardized malicious code provides instructions of the malicious code identified as to execution order.

15. The computer program of claim 1 wherein the library of standardized malicious code expresses instructions of the malicious code as standard synonym instructions.

16. The computer program of claim 1 wherein the library of standardized malicious code wherein the standardized version removes irrelevant program portions from the malicious code.

17. The computer program of claim 1 wherein the detector portion outputs a representation of the malicious portion when a malicious portion is present in the suspect program.